

A FOUNDATIONAL FRAMEWORK FOR A *PRIVACY BY DESIGN* PRIVACY IMPACT ASSESSMENT

Privacy by ReDesign: A Transformative Process

A Pre-Conference Seminar of the 33rd International
Conference of Data Protection and Privacy Commissioners

Pat Jeselon
President

Anita Fineberg
Barrister & Solicitor

Pat Jeselon & Associates Consulting Inc.

Pat Jeselon &

AGENDA

1. Purpose
2. Scope & Unique Features
3. Overview
4. Principle
5. Conclusion

Respect for the Individual

Privacy by Design Principles

Pro-Active

Privacy as Default

Embed into Design

Visibility and Transparency

End-to-End Security Lifecycle

Privacy by Design Applications

Accountable Business Practices

Physical Design and Infrastructure

Information Technology

= Positive-Sum

PURPOSE OF THE FRAMEWORK

- Operationalizes the holistic philosophy of *PbD*:
 1. Encourages organizations to adopt the *PbD* Principles into all aspects of their operations wherever and whenever personal information (PI) is collected, used, disclosed, retained, transferred, and/or disposed of
 2. Offers a practical guide to direct and inform decisions in the design of Applications:
 - information technology,
 - business processes, and
 - physical spaces and networked infrastructures
 3. Enables organizations to achieve positive-sum outcomes / win-win solutions for Application design

FRAMEWORK'S SCOPE & UNIQUE FEATURES

- Offers an approach that is broader than PIAs which focus primarily on an organization's statutory compliance and FIPs
- Adopts a user-centric approach that ensures privacy protection is embedded into Applications from the outset
- Encourages organizations to consider and respect the privacy expectations of the individuals regarding their PI in every aspect of an organization's operations
- Applicable in both private and public sector environments

FRAMEWORK'S SCOPE & UNIQUE FEATURES (CONT'D)

- Flexible enough to accommodate:
 - local legislation and regulatory requirements,
 - customization of political, technical and industry requirements, and
 - client and stakeholder privacy expectations
- Ensures a comprehensive assessment of the governance of and accountability for PI by considering an organization's privacy and data protection practices in their entirety
- Clearly assesses privacy and data protection practices and controls present in an organization's Applications

FRAMEWORK OVERVIEW

- Each *PbD* Principle is individually addressed through a series of questions designed to assist in the PIA analysis within the context of the reader's local environments
 - relevance and/or 'weight' of each principle may vary depending on the nature of the industry or Application being analyzed
- Questions speak to all three Applications
 - where appropriate, additional questions specific to one, or more, of the Applications are added
- Potential benefits that may accrue to the organization as a result of conducting a *PbD* PIA are identified

PRINCIPLE 2: PRIVACY AS THE DEFAULT SETTING

- *PbD* seeks to deliver the maximum degree of privacy by ensuring that PI is automatically protected in any given Application.
No action is required on the part of individuals to protect their privacy—privacy protection is built into the Application by default.

APPLICATIONS' QUESTIONS

Principle 2: Privacy as the Default Setting

- Do you design information technologies, business processes, physical spaces, and networked infrastructures around the principles of minimizing the identifiability, observability, and linkability of PI to the greatest degree possible?
- Do you ensure that the purposes for which PI is collected, used, and disclosed are clear, limited and relevant to the circumstances?
- Do you ensure PI is collected, used, and disclosed according to the stated purposes for its collection, use, and disclosure?
- Do you collect, use, and disclose PI only if other information would not serve the purpose?
- Have policies and procedures been developed and implemented that require the use of encrypted, de-identified or aggregate information rather than PI where PI is not necessary to serve the purpose?
- Do these policies and procedures require the encryption of all PI collected, used and disclosed using mobile devices?
- Do you collect, use, and disclose the minimum amount of PI necessary to serve the purpose?
- Have you implemented user access controls based on 'need to know,' and 'least privilege' principles? Does access control extend to technical staff?

SPECIFIC QUESTIONS & BENEFITS

Application-Specific Questions

| Information Technology | Accountable Business Processes | Physical Design and Networked Infrastructure |
|--|--------------------------------|--|
| Have policies and procedures been developed to outline the acceptable use of information technologies? | | |

Principle 2: Benefits to the Organization

- Reassures the individual whose PI is being collected, used, and disclosed that appropriate privacy controls and practices were implemented.
- Ensures individuals are made aware of their privacy rights and how they can exercise them, which, in turn, builds trust.

CONCLUSION

- The *PbD* Principles are considered in each of the Applications to ensure that a holistic approach to the PIA analysis is taken.
- The Framework ensures that the completed PIA captures
 1. the entire scope of an organization's privacy and data protection program, and
 2. the design and functionality of information technologies, business processes, physical spaces and networked infrastructures.

CONTACT INFORMATION

Pat Jeselon

(647) 287-6154 (B)

pjeselon@patjeselon.com

<http://www.patjeselon.com>

Anita Fineberg

416.762.4583 (B)

416.565.5007

afineberg@sympatico.ca

<http://www.linkedin.com/in/anitafineberg>